

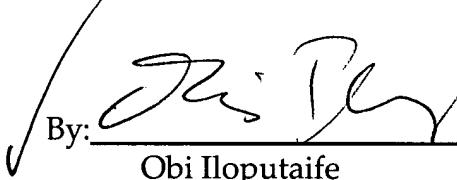
REMARKS

Claims 198-240 are pending in the present patent application. The Examiner rejects claims 228-240 and indicates claims 198, 199 and 201-227 are allowable. Applicant cancels rejected claims 228-240 in this response and previously cancelled claim 200 in the response dated October 24, 2002. The only pending claims are the claims the Examiner indicated were allowable. Applicant therefore respectfully requests allowance of the present application.

Respectfully submitted,

THE HECKER LAW GROUP

Date: April 7, 2003

By: 

Obi Iloputaife  
Reg. No. 45,677

THE HECKER LAW GROUP  
1925 Century Park East  
Suite 2300  
Los Angeles, California 90067  
(310) 286-0377

**CERTIFICATE OF MAILING**

*This is to certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Assistant Commissioner for Patents, Washington, D.C. 20231 on April 7, 2003.*

 4-7-03

Signature: Deanna Blizzard Date: April 7, 2003.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

**CLAIMS**

What is claimed is:

1 – 197. (CANCELLED)

198. (ONCE AMENDED) A system for transferring items having value ~~secure processing of value bearing items~~ in a computer network comprising:

a plurality of user terminals coupled to a computer network;  
a database system coupled to said network and remote from said plurality of user terminals for storing information about one or more users using said plurality of user terminals; and

a server system coupled to said network, said server system comprising a cryptographic device capabilities for transferring an item having value ~~performing secure [VBI] functions~~ utilizing said information stored in said database system.

199. (ONCE AMENDED) The system of claim 198, further comprising a plurality of postal security device data stored in said database system for ensuring authenticity of each of said one or more users, wherein each postal security device data is related to one of said users and said postal security device data related to said one of said

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

users is loaded into said associated with said cryptographic device capabilities when said one of said users requests to print said item having value a value bearing item.

200. (PLEASE CANCEL WITHOUT PREJUDICE)

201. (ONCE AMENDED) The system of claim 198, wherein said database system comprises data for creating indicium, account maintenance, and revenue protection.

202. (ONCE AMENDED) The system of claim 198, wherein said item having value value bearing item is a mail piece.

203. (ONCE AMENDED) The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device generates a digital signature in response to a user request for printing a value-bearing item said item having value.

204. (ONCE AMENDED) The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a said cryptographic device that encrypts the requested information in response to a user request for printing a value-bearing item said item having value.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

205. (ONCE AMENDED) The system of claim 202, wherein said server system comprising said cryptographic capabilities further comprises a said cryptographic device that generates data sufficient to print a postal indicium in compliance with postal service regulations on said mail piece.

206. (ONCE AMENDED) The system of claim 198, wherein said value-bearing item item having value is comprises a ticket.

207. (ONCE AMENDED) The system of claim 198, wherein a bar code is printed on said value-bearing item item having value.

208. (ONCE AMENDED) The system of claim 198, wherein said value-bearing item having value is comprises a coupon.

209. (UNCHANGED) The system of claim 199, wherein said postal security device data comprises an ascending register value, a descending register value, a respective cryptographic device ID, and an indicium key certificate serial number.

210. (ONCE AMENDED) The system of claim 199, wherein said postal security device data comprises a private key, a public key, and a public key certificate, wherein said private key is used to sign device status responses and said value-bearing

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

item having value which, in conjunction with said public key certificate, demonstrates that said postal security device and said ~~value-bearing~~ item having value are authentic.

211. (UNCHANGED) The system of claim 210, wherein said private key is used to sign device status responses.

212. (ONCE AMENDED) The system of claim 210, wherein said ~~value-bearing~~ item having value in conjunction with said public key certificate, authenticates said postal security device and said ~~value-bearing~~ item having value.

213. (ONCE AMENDED) The system of claim 198, wherein said cryptographic capabilities comprises a cryptographic device and said cryptographic device protects data using a stored secret.

214. (UNCHANGED) The system of claim 213, wherein said secret is a password.

215. (UNCHANGED) The system of claim 213, wherein said secret is a public and private key pair.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

216. (ONCE AMENDED) A method for secure processing of ~~value-bearing~~ items having value (VBIs) in a computer network comprising a plurality of user terminals comprising:

storing information about one or more users using a plurality of user terminals in a database system coupled to a network and remote from said plurality of user terminals; and

performing secure VBI functions for an item having value utilizing said information stored in said database system ~~by a to execute~~ cryptographic device capabilities remote from said plurality of user terminals.

217. (ONCE AMENDED) The method of claim 216 further comprising storing a plurality of postal security device data in said database system, wherein each of said security device data is related to one of said users.

218. (ONCE AMENDED) The method of claim 217 further comprising loading a postal security device data related to said cryptographic device capabilities when said one of said users requests to print a ~~value-bearing~~ said item having value.

219. (UNCHANGED) The method of claim 216 further comprising authenticating the identity of each user.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

220. (ONCE AMENDED) The method of claim 219 further comprising verifying that the identified user is authorized to print ~~a value bearing~~ said item having value.

221. (ONCE AMENDED) The method of claim 216, wherein said the value bearing item having value is a mail piece.

222. (ONCE AMENDED) The method of claim 216, wherein said cryptographic capabilities are provided by said a cryptographic device configured to generates a digital signature in response to a user request for printing ~~said a value bearing~~ item having value.

223. (ONCE AMENDED) The method of claim 216, wherein said cryptographic capabilities comprises said a cryptographic device configured to encrypts the requested information in response to a user request for printing ~~said a value bearing~~ item having value.

224. (ONCE AMENDED) The method of claim 221, wherein cryptographic capabilities comprises a said cryptographic device configured to generates data sufficient to print a postal indicium compliance with postal service regulations on said mail piece.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

225. (ONCE AMENDED) The method of claim 216, wherein said ~~value-bearing~~ item having value is a ticket.

226. (ONCE AMENDED) The method of claim 216, wherein a bar code is printed on said ~~value-bearing~~ item having value.

227. (ONCE AMENDED) The method of claim 216, further comprising printing a coupon.

228. (UNCHANGED) A method for secure processing of a value bearing item on a computer network having a plurality of users using a plurality of computer terminals for connecting to said network and a plurality of cryptographic devices remote from said plurality of users and coupled to said network, each cryptographic device executing a plurality of postal security device transactions, the method comprising:

requesting by a user authorization for printing a value bearing item;  
assigning a postal security device data to the requesting user, wherein said postal security device data may be executed on any of said plurality of cryptographic devices;

authenticating the identity of said user;

granting the requested print if the identity of said user is authenticated; and

printing said value-bearing item.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

229. (UNCHANGED) The method of claim 228, further comprising storing data for creating indicium, account maintenance, and revenue protection.

230. (ONCE AMENDED) The method of claim 228, wherein said the value-bearing item is a mail piece.

231. (ONCE AMENDED) The method of claim 228, wherein said cryptographic device generates a digital signature in response to a user request for printing said a value-bearing item.

232. (ONCE AMENDED) The method of claim 228, wherein said cryptographic device encrypts the requested information in response to a user request for printing said a value-bearing item.

233. (UNCHANGED) The method of claim 230, wherein said cryptographic device generates data sufficient to print a postal indicium in compliance with postal service regulations on said mail piece.

234. (UNCHANGED) The method of claim 228, wherein said value-bearing item is a ticket.

**Marked Up Copy Of The Claims In Accordance With 37CFR §1.121(c)(1)(ii)**

235. (UNCHANGED) The method of claim 228, wherein a bar code is printed on said value-bearing item.

236. (UNCHANGED) The method of claim 228, further comprising printing an image.

237. (UNCHANGED) The method of claim 228, wherein said postal security device data comprises an ascending register value, a descending register value, a respective cryptographic device ID, and an indicium key certificate serial number.

238. (UNCHANGED) The method of claim 228, further comprising using a private key to sign device status responses and said value-bearing item which, in conjunction with a public key certificate, demonstrates that said postal security device and said value-bearing item are authentic.